INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/06365

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F15/00 , H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-1999
Kokai Jitsuyo Shinan Koho 1971-1999 Toroku Jitsuyo Shinan Koho 1994-1999

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPI, INSPEC, "(proxy+server)*cipher"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP, 8-335207, A (Hitachi, Ltd.), 17 December, 1996 (17.12.96), page 2, left column, lines 2-43 (Family: none)	1,2,4,8-10 3,6,7
X	K. Takaragi et al.,"Firewall Internet Technology Relating to Firemall (in Japanese)", Tokyo: Shokodo, 10 June,1998 (10.06.98)p148-152	1,2,4,8-10
Y	JP, 7-212353, A (Nippon Yunishisu K.K.), 11 August, 1995 (11.08.95), page 5, left column, lines 24-45 (Family: none)	3
Y	Naomasa, Minami et al., "Research on the Development of the Platform for Self-decoding type Confidential Information Communication (in Japanese)", Symposium on Cipher and Information Security in 1996, 1996, SCIS96-01C	6,7
A	JP, 63-220630, A (Matsushita Electric Ind. Co., Ltd.), 13 September, 1988 (13.09.88), page 3; upper right column; lines 4 to 15 (Family: none)	6

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 February, 2000 (09.02.00)	29 February, 2000 (29.02.00)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/06365

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US, 5310999, A (AT&T BELL LAB.), 10 May, 1994 (10.05.94), Full text & EP, 577328, A2 & JP, 6-060237, A & DE, 69321166, E	6

国際調査報告

国際出願番号　PCT／JP99／06365

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷　G06F15／00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷　G06F15／00 , H04L9／32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1926－1996
日本国公開実用新案公報	1971－1999
日本国実用新案登録公報	1996－1999
日本国登録実用新案公報	1994－1999

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

WPI, INSPEC,　「(proxy+server)＊cipher」

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP8－335207, A（株式会社日立製作所）, 17. 12月. 1996（17. 12. 96）, 第2頁左欄第2－43行（ファミリーなし）	1, 2, 4, 8－10
Y		3, 6, 7
X	宝木和夫; 小泉稔, 寺田真敏, 萱島信,「ファイアウォール インターネット関連技術について」, 東京：昭晃堂, 10. 6月. 1998（10. 06. 98）p148－152	1, 2, 4, 8－10
Y	JP7－212353, A（日本ユニシス株式会社）, 11. 8日. 1995（11. 08. 95）, 第5頁左欄第24－45行（ファミリーなし）	3
Y	南尚鎮, 岡本栄司, 篠田陽一, 満保雅浩.「自己復号型秘密情報通信のためのプラットホームの開発研究」1996年暗号と情報セキュリティシンポジウム, 1996, SCIS96－01C	6, 7

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 09. 02. 00	国際調査報告の発送日　29.02.00
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 石井　茂和　印　5M　8837 電話番号　03－3581－1101　内線　6438

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ９９／０６３６５

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	ＪＰ，６３－２２０６３０，Ａ（松下電器産業株式会社），１３．９月．１９８８（１３．０９．８８），第３頁，右上欄，第４－１５行（ファミリーなし）	６
Ａ	ＵＳ，５３１０９９９，Ａ（ＡＴ＆Ｔ　ＢＥＬＬ　ＬＡＢ．）１０．５月．１９９４（１０．０５．９４）全文＆ＥＰ，５７７３２８，Ａ２＆ＪＰ，６－０６０２３７，Ａ＆ＤＥ，６９３２１１６６，Ｅ	６

明　細　書

ネットワーク認証装置および方法

技　術　分　野

本発明は、インターネット等の商用ネットワークにおけるセキュリティ技術に関する。

背　景　技　術

インターネットが商用目的で使用されるようになってくると、ネットワークのセキュリティ技術の早急な確立が必要になってきている。

すなわち、インターネットはＴＣＰ／ＩＰによるオープンなプロトコルを用いたデータ通信であり、データ通信の秘密性は本来的に予定されていない。

そのため、公開鍵等の各種の暗号化技術を用いてユーザー端末とサーバとの間のデータセキュリティを確保する技術が多数提案されている。

このような暗号通信では、ユーザー端末から暗号化された特定のデータをサーバに送信し、サーバではこれを復号化して当該ユーザーの正当性を認証するものが一般的であった。

しかし、前記認証サーバそのものはインターネット上でオープンな環境に配置されており、サーバそのものはファイアウォールが確立されていたとしても、そのサーバのアドレスは誰でも知ることができる状態だった。

すなわち、認証サーバは、そのアドレスが公知なことにより、常にハッカーやクラッカーの標的となってしまう可能性を否定できなかった。

さらに、悪意の第三者がこのような暗号化通信を傍受してサーバとの間でデータ通信を再開することにより、いわゆるなりすましが可能となり、クレジットカード等がネットワーク上で不正に使用されてしまう可能性もあった。

本発明は、このような点に鑑みてなされたものであり、認証サーバの存在その

ものの秘密性を高めるとともに、ユーザーが認証のためのデータ入力を行うプログラム自体を使い切り形式にしてユーザー端末に配信することにより、高いネットワークセキュリティを保証するシステムを提供することを技術的課題とする。

発　明　の　開　示

本発明の第１の手段は、データを入力するユーザー端末に対して、当該データを仲介する仲介サーバと、当該データに対して認証を与える認証サーバとからなり、前記ユーザー端末での第１のデータ入力を契機として、暗号化情報を仲介サーバに出力する認証サーバと、前記認証サーバから受信した暗号化情報に基づいて、前記ユーザー端末で入力される第２のデータを暗号化するための暗号化プログラムを生成し、この暗号化プログラムを前記ユーザー端末に配信する仲介サーバとからなるネットワーク認証装置である。

本発明の特徴はこのように「仲介認証システム」を実現した点にある。

すなわち、仲介サーバを経由させることにより、認証サーバの秘匿性を高めることができる。すなわち、認証サーバのアドレスそのものを秘密に保つことができる。

また、認証サーバが有する暗号化情報を仲介サーバに提供し、仲介サーバではこの固有の暗号化情報に基づいて暗号化プログラムを生成し、ユーザー端末から第２のデータが入力されるときに当該暗号化プログラムを通じて暗号化させる。ここで、暗号化プログラムは、ＪＡＶＡのアプレットで生成することができる。

なお、ユーザー端末とは、パーソナルコンピュータ等の屋内に設置する形式の端末装置に限らず、携帯電話に接続されて端末機能を有するモバイルコンピュータ、ＰＤＡ（Personal Data Assistant）等であってもよい。また、インターネット端末機能を有する携帯電話（ＮＴＴドコモ株式会社の「ｉモード端末」等）そのものであってもよい。

本発明の第２の手段は、前記第１の手段において、暗号化情報は暗号化関数とし、前記認証サーバは、暗号化プログラムにより暗号化された第２のデータと、自身が保有する第２のデータを前記暗号化関数で暗号化したものと比較することにより前記ユーザー端末からのセッションの正当性を評価するようにした。

暗号化関数は必ずしも一通りでなくてよく、複数の関数を用意しておくことにより、暗号化による秘匿性がより高められる。

本発明の第３の手段は、前記第１または第２の手段において、暗号化情報は、前記ユーザー端末から仲介サーバへのセッション毎に変化するようにした。

たとえば、認証サーバの機械時計の日時情報をパラメータ（変数）として用いることにより、セッション毎に異なる暗号化情報を生成することができる。これにより、ユーザー端末からのデータを傍受した第三者が不正に仲介サーバにアクセスしても、既に暗号化情報が変化しているために、認証サーバによる正当な認証を受けることができず、秘密が保たれる。

本発明の第４の手段は、前記第１の手段において、前記第１のデータはユーザーＩＤであり、第２のデータはパスワードであることとした。たとえばクレジットカードの獲得ポイント数の確認等において、高い秘匿性が要求されるパスワード情報の転送に本発明を用いることができる。

本発明の第５の手段は、前記第２の手段において、暗号化情報として前記認証サーバのかわりに、前記仲介サーバが有する複数の暗号化関数の中から暗号化関数を特定する暗号化キーにしたものである。

この場合には、認証サーバと仲介サーバとに同一の関数テーブルを有しており、当該暗号化キーによってテーブル中から採用する暗号化関数を特定することができるようになっている。

本発明の第６の手段は、ユーザー端末より受信した第１のデータを仲介サーバにおいて認証サーバに仲介するステップと、前記第１のデータに基づいて暗号化情報を生成し、当該暗号化情報を仲介サーバに送信するステップと、前記第１のデータに対応し認証サーバが保有する第２のデータを読み出してこれを前記暗号化情報で暗号化するステップと、仲介サーバにおいて、前記暗号化情報に基づいて、前記ユーザー端末で入力される第２のデータを暗号化するための暗号化プログラムを生成し、この暗号化プログラムを前記ユーザー端末に配信するステップと、ユーザー端末において、前記暗号化プログラムによって入力された第２のデータを暗号化するステップと、ユーザー端末で暗号化された第２のデータを、前記認証サーバで暗号化された第２のデータと比較するステップとからなるネットワーク認証方法である。

本手段においても、仲介サーバを経由させることにより、認証サーバの秘匿性を高めることができる。すなわち、認証サーバのアドレスそのものを秘密に保つことができる。また、認証サーバが有する暗号化情報を仲介サーバに提供し、仲介サーバではこの固有の暗号化情報に基づいて暗号化プログラムを生成し、ユーザー端末から第２のデータが入力されるときに当該暗号化プログラムを通じて暗号化させる。ここで、暗号化プログラムは、ＪＡＶＡのアプレットで生成することができる。

本発明の第７の手段は、前記第６の手段において、前記暗号化情報を、前記ユーザー端末から仲介サーバへのセッション毎に変化させるようにした。

たとえば、認証サーバの機械時計の日時情報をパラメータ（変数）として用いることにより、セッション毎に異なる暗号化情報を生成することができる。これにより、ユーザー端末からのデータを傍受した第三者が不正に仲介サーバにアクセスしても、既に暗号化情報が変化しているために、認証サーバによる正当な認証を受けることができず、秘密が保たれる。

本発明の第８の手段は、前記第６の手段で述べたステップからなるプログラムを記憶した記憶媒体である。

ここで、記憶媒体とは、光学的、磁気的、光磁気的な記録手段を備えたあらゆる媒体を含み、光ディスク、光磁気ディスク、磁気テープ、またはこれらを収容したカートリッジ、カセット、カード等を含む。

本発明の第９の手段は、認証サーバはユーザー端末での処理要求の入力を契機にこの処理要求に対する固有情報を発生させ、これを受け取った仲介サーバは、前記固有情報に基づいて生成した入力インターフェースを前記ユーザー端末に提供するものである。

処理要求とは、たとえばインターネットブラウザ等に表示されるボタンをユーザーがマウスで指示することにより送信される行為を意味する。認証サーバで発生させる固有情報とは、たとえば当該処理要求に対応する受付番号や暗号化方法等を意味する。

本発明の第１０の手段は、前記第９の手段において、前記入力インターフェースとしてユーザー端末上で機能する実行プログラムを用意し、この実行プログラ

ムでは２以上のユーザー情報の入力を受け付けてこれらを暗号化して前記仲介サーバに送信するようにしたものである。

実行プログラムとは、たとえばＪＡＶＡアプレットであり、ユーザー情報とはこのアプレット上で入力されるカード番号や暗証番号を意味する。これらのユーザー情報は、当該アプレット上で暗号化されて仲介サーバを経て認証サーバに送られる。

図面の簡単な説明

図１は、本発明の実施形態におけるシステム構成を示す概略図

図２は、受付データベースの内容を示す説明図

図３は、オーソリデータベースの内容を示す説明図

図４は、実施形態の受付処理における仲介サーバと認証サーバの機能ブロック図

図５は、実施形態の認証処理における仲介サーバと認証サーバの機能ブロック図

図６は、実施形態において、ユーザー端末に提供されるＨＴＭＬファイルと暗号化アプレットの生成手順を示すブロック図

図７は、実施形態において、ユーザー端末に提供されるＨＴＭＬファイルのソースコードを示す説明図

図８は、実施形態の仲介サーバでの暗号化アプレットの生成方法の変形例を示すブロック図

図９は、実施形態の暗号化テーブルを示す説明図（１）

図１０は、実施形態の暗号化テーブルを示す説明図（２）

図１１は、実施形態の暗号化テーブルを示す説明図（３）

図１２は、実施形態のアプレットのテンプレートを示す説明図

図１３は、実施形態においてユーザー端末と仲介サーバと認証サーバとの間のデータのやりとりを示すシーケンス図

図１４は、実施形態のユーザー端末の表示画面（１）

図１５は、実施形態のユーザー端末の表示画面（２）

図１６は、実施形態のユーザー端末の表示画面（３）

図１７は、実施形態のユーザー端末の表示画面（４）

図１８は、実施形態の変形例におけるユーザー端末と仲介サーバと認証サーバとの間のデータのやりとりを示すシーケンス図（１）

図１９は、実施形態の変形例におけるユーザー端末と仲介サーバと認証サーバとの間のデータのやりとりを示すシーケンス図（２）

発明を実施するための最良の形態

以下本発明を図面に基づいて説明する。

図１は、本実施形態のシステム構成を示す概略図である。

本実施形態は、ユーザー端末１がインターネット２を介して仲介サーバ３に接続されており、この仲介サーバ３はファイアウォールサーバ４を介してＬＡＮまたはＷＡＮによって認証サーバ５と接続されている。

このユーザー端末１は、パーソナルコンピュータ等の屋内に設置する形式の端末装置に限らず、携帯電話に接続されて端末機能を有するモバイルコンピュータ、ＰＤＡ（Personal Data Assistant）等であってもよい。また、インターネット端末機能を有する携帯電話（ＮＴＴドコモ株式会社の「ｉモード端末」等）そのものも用いることができる。

認証サーバ５は、受付データベース６とオーソリデータベース７とを有しており、各データベースのファイル構成は図２および図３に示す通りとなっている。すなわち、受付データベース６には、認証サーバ５で付与される受付番号と、ユーザー端末１で入力されたカード番号と、暗号化アルゴリズムを特定するための暗号化キー（後で詳述する）が登録されている。また、オーソリデータベース７には、認証のためにあらかじめ登録されているカード番号と、同じくあらかじめ登録されているパスワードとが登録されている。

なお、認証サーバ５には、前記受付データベース６とオーソリデータベース７以外にも、ユーザー情報データベース２６および認証結果データベース２７（ともに図５参照）を有しているが、図１では図示を省略している。

前記図１に示したシステムは、たとえば、ユーザーが、ユーザー端末１よりクレジットカードの番号およびパスワードを入力することにより、当該クレジット

カードに累積されたポイント（得点）を参照するために用いられる。ユーザー端末１から入力されるクレジットカード番号やパスワードは、通信路上で高いセキュリティが必要であり、またこれを認証するための認証サーバ５も受付データベース６やオーソリデータベース７のセキュリティを維持する必要がある。

本実施形態では、これらの点について、ユーザー端末１から入力されるクレジットカード番号やパスワードを一時的な使い切りプログラム、たとえば使い捨てのＪＡＶＡアプレットを用いて通信路上のデータ傍受を防止するとともに、仲介サーバ３を設けてユーザー端末１は直接的にはこの仲介サーバ３と交信することにより、認証サーバ５そのもののアドレスやシステム構成を秘密化している。

次に、図４を用いてユーザー端末１と仲介サーバ３と認証サーバ５のそれぞれの機能について説明する。

図４は、ユーザー端末１が仲介サーバ３のサーバプログラム１２にアクセスして（図１４参照）、カード番号入力画面（図１５参照）を選び、カード番号を仲介サーバ３に送信し、図１６に示した暗証番号入力画面がユーザー端末１に表示されるまでのユーザー端末１と仲介サーバ３と認証サーバ５との各機能分担を示したブロック図である。

まず、ユーザーは、ユーザー端末１よりインターネット２にダイヤルアップＩＰ等の方法でアクセスし、ユーザー端末１内のブラウザ１１（WWW閲覧プログラム）を起動する。そして、ＵＲＬ(Uniform Resource Locator)として仲介サーバ３のサーバプログラム１２のアドレスを指定することによって、図１４に示す画面が表示される。

そして、ユーザーが図１４に示した画面上でポイント照会をマウス等の入力補助装置を用いて指定することによって、当該「ポイント照会」に設定されたリンク情報にしたがって、図１５に示すカード番号入力画面が表示される。

ここで、ユーザーが自身のカード番号（たとえば「１２３４」）を入力すると、この入力されたカード番号（ＩＤ）が仲介サーバ３に送信される（図４のステップ(1)：以下、本実施態様におけるカッコ付き数字は、図４の丸付き数字に対応する）。

仲介サーバ３のサーバプログラム１２が前記カードＩＤを受け取ると、受付サーブレット１３（使い切りのサーバ側プログラム）を起動して（ステップ(2)）、

カードＩＤを受付サーブレット１３を介してキューイング１４の状態にする（ステップ(3)，(4)）。

認証サーバ５は、キューフェッチ機能１５により仲介サーバ３からのキューを定期的にチェックしており（ステップ(5)）、前記キュー１４を確認するとこれを取り込む（ステップ(6)）。

そして、認証サーバ５は、オーソリ・ユーザー・エージェント・プログラム（以下、「オーソリＵＡ」という）１６を起動するとともに、このオーソリＵＡ１６に対してカードＩＤを送信する（ステップ(7)，(8)）。このオーソリＵＡ１６は一時的なエージェント・プログラムであり、ユーザー端末１よりなんらかの理由で通信が切断された場合には、一定時間経過後に認証サーバ５上から削除される。

オーソリＵＡ１６は、さらに、認証サーバ５の暗号化関数管理部１７より暗号化キーと暗号化関数を読み出して（ステップ(9)）、受付番号を生成し、受付情報を受付データベース６に格納する（ステップ(10)）。なお、暗号化キーとは、暗号化するための鍵情報を意味し、複数の暗号化関数の中からアクセス毎に択一的に採用されたものを用いる。

このような暗号化キーを用意しておく理由は以下の通りである。

すなわち、カードＩＤは一定であるため、同一のカードＩＤで複数回のアクセスがあることが考えられる。そのため、カードＩＤに対してアクセス毎に異なる暗号化キーを実現できる複数の暗号化関数を用意しておくことにより、不正アクセスを防止できる。

なお、暗号化キーと暗号化関数については、図９，１０および１１を用いて後述する。また、受付番号は、シーケンシャルな番号であり、毎日午前零時にリセットされる。すなわち、その日の３番目のアクセスには「０００３」が付与される。

オーソリＵＡ１６は、前記のように受付順に付与される受付番号を生成し（ステップ(10)）、前記カードＩＤと暗号化キーとともに受付データベース６に格納する（図２参照）。

次に、オーソリＵＡ１６は、仲介サーバ３対して仲介ユーザー・エージェント（以下、「仲介ＵＡ」という）２０の起動を指示する（ステップ(11)，(12)）。

仲介サーバ３内で仲介ＵＡ２０が起動されると、前記認証サーバ５のオーソリＵＡ１６から受付番号、カードＩＤ、暗号化関数からなる受付情報を送信する（ステップ(13)）。

この受付情報を受け取った仲介ＵＡ２０は、前述の受付サーブレット１３に対して受付番号と暗号化関数を送信する（ステップ(14)）。

受付サーブレット１３は、これに基づいて、受付番号と暗号化関数を埋め込んだ暗号化アプレット２１を生成する（ステップ(15)）。この暗号化アプレット２１はサーバプログラムを通じてユーザー端末１のブラウザ１１に送信される（ステップ(16), (17)）。

この暗号化アプレット２１とは、いわゆるＪＡＶＡアプレットであり、インターフェースとしてのＨＴＭＬ(Hyper Text Mark-up Language)ファイルとともにユーザー端末１のブラウザ１１に送信される。このときのブラウザ１１の画面を示したものが図１６である。これを表示するためのＨＴＭＬファイルは、図７に示すようにテキストの記述で構成されている。この記述中、APPLET CODEとして指定されているOTP19980812114910.classが暗号化アプレット２１のファイル名となっている。この暗号化アプレット２１は、いわゆるワン・タイム・プログラムであり、当該カードＩＤの認証のためのセッションのみに用いられる一時的なプログラムである。暗号化アプレット２１は、前述のように、認証サーバ５で付与された受付番号と、暗号化関数によって生成されているため、同一の暗号化アプレット２１が生成される可能性は天文学数値的に低くなっている。

次に、図５を用いて、ユーザー端末１のブラウザ１１上で、図１６に示したアプレット画面で入力されたパスワードが、仲介サーバ３を経由して認証サーバ５で認証されて図１７に示すような認証画面が表示されるまでの仲介サーバ３と認証サーバ５との機能を説明する。

まず、ユーザー端末１上のブラウザ１１より入力されたパスワードは、前述のように１回のセッションだけのために生成された前記暗号化アプレット２１によって暗号化されて仲介サーバ３に送信される（ステップ(2)）。このように仲介サーバ３から提供された１回限りの暗号化アプレット２１を用いて入力されたパスワードを暗号化することによって、ユーザー端末１と仲介サーバ３との回線をトレースして当該通信を傍受したとしても、同一のカードＩＤによる次のセッショ

ンには利用することができない。

前記暗号化パスワードを受信した仲介サーバ３では、サーバプログラム１２によって認証サーブレット２５が起動され、ここに前記暗号化パスワードが引き渡される（ステップ(3)，(4)）。

ここで、認証サーブレット２５は、図４で説明した受付サーブレット１３が保有していた受付番号を引き継ぎ、暗号化パスワードとともにこの受付番号を仲介ＵＡ２０に送信する（ステップ(5)）。

認証サーバ５のオーソリＵＡ１６からは一定間隔で仲介サーバ３に対して認証要求がなされており（ステップ(1)）、仲介サーバ３の仲介ＵＡ２０が前述の受付番号と暗号化パスワードを受け取った状態になっていると、この認証要求をトリガとしてこれらの情報をオーソリＵＡ１６に送信する（ステップ(6)）。

オーソリＵＡ１６は、前記受付番号をキーにして受付データベース６にアクセスし、この受付番号に対応するカードＩＤと暗号化キーを読み出す（ステップ(7)）。そして、得られたカードＩＤと暗号化キーと前記の暗号化パスワードを組にして認証部２８に対して認証要求を行う（ステップ(8)）。

前記認証要求を受け付けた認証部２８は、暗号化関数管理部１７より暗号化関数を読み出すとともに（ステップ(9)）、オーソリデータベース７よりカードＩＤをキーにしてパスワードを読み出す（ステップ(10)）。そして、認証部２８は、オーソリデータベース７から読み出したパスワードを暗号化関数によって暗号化し（ステップ(11)）、これをオーソリＵＡ１６が受信した暗号化パスワードと比較する（ステップ(12)）。

認証部２８は、前記両暗号化パスワードが一致した場合には、認証ＯＫとして、ユーザー情報データベース２６よりユーザー情報を読み出す（ステップ(13)）。このユーザー情報とは、たとえば当該ユーザーのクレジットカードに対する獲得ポイント数などである。　そして、認証部２８は、認証結果データベース２７にこの認証結果として、受付番号、暗号化パスワードおよびユーザー情報を登録する（ステップ(14)）。これとともに、オーソリＵＡ１６に対して認証結果、すなわち認証ＯＫの結果フラグと獲得ポイント数等のユーザー情報を送信する（ステップ(15)）。

オーソリＵＡ１６は、認証結果がＯＫだった場合には、受付データベース６に

暗号化パスワードを書き込むとともに（ステップ(16)）、仲介サーバ３の仲介ＵＡ２０に対して認証結果をユーザー情報とともに送信する（ステップ(17)）。

前記認証結果は、仲介サーバ３の仲介ＵＡ２０→認証サーブレット２５およびサーバプログラム１２を経由してユーザー端末１に送信され、当該ユーザー端末１上のブラウザ画面に表示される（ステップ(18)～(20)）。

このときのユーザー端末１上の表示画面を示したものが図１７である。

次に、図４で説明したブラウザ１１に提供されるＨＴＭＬファイルと暗号化アプレット２１の生成手順について図６を用いて説明する。

まず、前述のように、ブラウザ１１上よりカードＩＤが入力されると（ステップ(1)）、サーバプログラム１２が起動し、受付サーブレット１３の起動が促される（ステップ(2)）。

受付サーブレット１３は、まず、図１２に示すようなアプレットのテンプレート６１を選択的に読み出して（ステップ(3)）、種プログラム(Seed)の書き換えと実行ファイル(class)の出力を行い（ステップ(4)）、暗号化アプレット２１を生成する。そして、この暗号化アプレット２１は、受付サーブレット１３によって生成されたＨＴＭＬデータ６２とともに、サーバプログラム１２を通じてユーザー端末１のブラウザ１１に提供される（ステップ(5)～(6)）。

このＨＴＭＬデータ６２の具体的なソースコードを示したものが図７である。

次に、本実施形態における暗号化について説明する。

まず、前記暗号化アプレット２１を当該セッション限りの使い切りとするため、暗号化キーを設定する。すなわち、暗号化キーの操作によってセッション毎に異なる暗号化式を生成させることになる。そのため、暗号化関数管理部１７には、図９および図１０に示す暗号化関数を登録した暗号化テーブルＡおよびＢが設けられている。

すなわち、本実施形態では、暗号化キーによって採用される暗号化関数が特定されるようになっており、この暗号化キーは後の認証のために認証サーバ５の受付データベース６内に保持される（図５参照）。

図９および図１０において、変数ａは日付であり、各サーバが有している時計機能から得る。当該テーブル構成において、暗号化キーとして「Ａ３」が指定されたときには、図９に示すテーブルＡの３番目の式、すなわち、「Ｙ＝ａＸ＋３」

が採用される。この式を用いた場合、たとえば当該日が１０日であるとすると（ａ＝１０）、入力された数値Ｘを１０倍して３を加えた数値Ｙが暗号化値となる。

なお、暗号化キーは、セッション毎に異なる数値が生成されるように、変数としてサーバの機械時計の値を用いてもよい。たとえば、暗号化テーブルに図１１に示すような関数が登録されている場合、Ａはサーバの機械時計の秒（４桁）、Ｂはサーバの機械時計の年月日（６桁）、Ｃはサーバの機械時計の時分（４桁）としてもよい。

次に、図１３を参照しながら、本実施形態における暗号化と認証の理解を容易にするために、以下の具体的な数値を用いてユーザー端末１と、仲介サーバ３と、認証サーバ５とのやりとりを時系列的に説明する。

カード番号（ＩＤ）：１２３４
受付番号：４９１２
パスワード：９１０４
暗号化関数：Ｙ＝３Ｘ－９９

まず、ユーザー端末１よりカード番号（ＩＤ）として「１２３４」が入力されると（ステップ１３０１）、仲介サーバ３はこれを仲介して（１３０２）、認証サーバ５に通知する。

認証サーバ５では、このカード番号（ＩＤ）「１２３４」を取得し、これに受付番号「４９１２」を付与する。そして、暗号化方法を設定する（１３０３）。具体的には暗号化関数「Ｙ＝３Ｘ－９９」とこの関数を特定する暗号化キーが暗号化関数管理部１７から読み出される（図４参照）。

仲介サーバ３は認証サーバ５より前記受付番号「４９１２」と暗号化関数「Ｙ＝３Ｘ－９９」を取得し（１３０４）、これらを埋め込んだ暗号化アプレット２１を生成する（１３０５）。

次に、ユーザー端末１上でパスワード「９１０４」が入力されると（１３０６）、これが暗号化関数「Ｙ＝３Ｘ－９９」によって計算され、計算結果が暗号化暗証番号「２７２１３」として仲介サーバ３を通じて認証サーバ５に通知される（１

３０７，１３０８）。

一方、認証サーバ５では、前記と並行して、前記暗号化関数「Ｙ＝３Ｘ－９９」を暗号化関数管理部１７から読み出すとともに（１３０９）、ステップ１３０３で取得したカード番号（ＩＤ）をキーにしてオーソリデータベース７よりパスワード「９１０４」を読み出す（１３１０）。そして、読み出されたパスワードを、前記暗号化関数「Ｙ＝３Ｘ－９９」によって暗号化する（１３１１）。そしてここで暗号化された数値と前述のユーザー端末１から通知された暗号化暗証番号「２７２１３」と比較する（１３１２）。

この結果、オーソリデータベース７に格納されていたパスワードを暗号化したものと、ユーザー端末１からの暗号化暗証番号とが一致した場合には認証が成立して認証サーバ５内で保持されていたユーザー情報が仲介サーバ３を介して（１３１３）、ユーザー端末１に提供される（１３１４）。

なお、以上の説明は認証サーバ５から暗号化関数を仲介サーバ３に通知して暗号化アプレット２１を生成する場合であったが、図８に示すように、仲介サーバ３が認証サーバ５から暗号化キー８０１のみを受け取り、仲介サーバ３自身が有する関数テーブル８０２との組み合わせで暗号化アプレット２１を生成してもよい。

この場合、仲介サーバ３が保持する関数テーブル８０２は、認証サーバ５が有する暗号化関数管理部１７の関数テーブルと同一のものでなければならない。

図１８は、本発明の実施形態の変形例におけるユーザー端末と仲介サーバと認証サーバとの間のデータのやりとりを示すシーケンス図である。

前述の図１３のシーケンス図では、ユーザー端末１よりカード番号を入力した後に認証サーバで受付番号が発行され、これに基づいて仲介サーバ３でアプレットが生成・配信され、ユーザー端末１上ではこのアプレット上で暗証番号を入力するようになっていた。

これに対して、図１８のシーケンスでは、ユーザー端末１で処理要求がなされると、認証サーバ５からの受付番号・暗号化方法に基づいて仲介サーバでアプレットが生成・配信され、ユーザー端末１上ではこのアプレット上でカード番号と暗証番号を入力するようになっている。

これを具体的に説明する。

まず、ユーザー端末１上でユーザーがインターネットブラウザ等を通して表示された処理要求のボタンをマウスでクリックすると（ステップ１８０１）、仲介サーバ３は、この処理要求があったことを認証サーバ５に通知する（１８０２）。認証サーバ５では、これに基づいて受付番号と暗号化方法（たとえば、暗号化関数「Ｙ＝３Ｘ－９９」）を設定する（１８０３）。このステップ１８０３の処理は前述の図１３のステップ１３０３と同様である。ここで、たとえば受付番号として４９１２が認証サーバ５に付与されたとすると、この受付番号と暗号化方法とが仲介サーバ３に通知される（１８０４）。

仲介サーバ３ではこれに基づいて、アプレットを生成しユーザー端末１に配信する（１８０５）。

ユーザー端末１上では、仲介サーバ３から配信されたアプレットが実行され、ユーザーからカード番号と暗証番号の入力を受け付ける（１８０６）。ここで、入力された暗証番号は、前述の暗号化方法に基づいてアプレット上で暗号化暗証番号（ここでは、Ｙ＝３Ｘ－９９＝３×９１０４－９９＝２７２１３）に変換されて仲介サーバ３に送られる（１８０７）。

一方、認証サーバ５では、前記と並行して、前記暗号化関数「Ｙ＝３Ｘ－９９」を暗号化関数管理部１７から読み出すとともに（１８０９）、対象となるデータをオーソリデータベース７より読み出す（１８１０）。これには、カード番号とパスワード「９１０４」が含まれる。そして、読み出されたパスワードを、前記暗号化関数「Ｙ＝３Ｘ－９９」によって暗号化する（１８１１）。そしてここで暗号化された数値と前述のユーザー端末１から通知された暗号化暗証番号「２７２１３」と比較する（１８１２）。

この結果、オーソリデータベース７に格納されていたパスワードを暗号化したものと、ユーザー端末１からの暗号化暗証番号とが一致した場合には認証が成立して認証サーバ５内で保持されていたユーザー情報が仲介サーバ３を介して（１８１３）、ユーザー端末１に提供される（１８１４）。

このように図１８に示した変形例では、ユーザーに対してカード番号と暗証番号を同じアプレット上で入力させるため、カード番号を入力してから暗証番号の入力画面を待つというようなユーザーにストレスを感じさせることがない。

また、図１８ではステッ・ｖ１８０６のアプレット上でカード番号と暗証番号の

２つのユーザー情報を入力する例を示したが、ユーザー情報はこれらの２つに限られず、複数の項目を入力させるようにしてもよい。この例をシーケンス図で示したものが図１９である。　同図に示すように、オーソリデータベース７には複数の項目のデータが登録されており、これらと入力されたユーザー情報が照合されることになる。

なお、詳細は図１３および図１８で説明したものと同様であるので説明は省略する。

以上説明したように、本発明によれば、ユーザー端末からの認証業務に対して、仲介サーバを経由することにより認証サーバの存在そのものを秘密化できる。

また、仲介サーバによって当該セッション限りの使い切りの暗号化プログラムを提供し、この暗号化プログラムによってユーザー端末上で入力データを暗号化できるため、通信路上での漏洩に対してもセキュリティの高いデータ通信が可能となる。

さらに、前記暗号化プログラムは当該セッション限りの使い切りの暗号化プログラムであるため、漏洩したデータに基づいて第三者がセッションを開始しても暗号化プログラムが一致することはなく、不正アクセスを防止できる。

産業上の利用可能性

本発明は、ユーザーが端末コンピュータや携帯端末からインターネットを経由した商品購入等の場合の認証システムに利用できる。

請 求 の 範 囲

1．データを入力するユーザー端末に対して、当該データを仲介する仲介サーバと、当該データに対して認証を与える認証サーバとからなり、

前記ユーザー端末での第１のデータの入力を契機に、暗号化情報を仲介サーバに出力する認証サーバと、

前記認証サーバから受信した暗号化情報に基づいて、前記ユーザー端末で入力される第２のデータを暗号化するための暗号化プログラムを生成し、この暗号化プログラムを前記ユーザー端末に配信する仲介サーバとからなるネットワーク認証装置。

2．前記暗号化情報は暗号化関数であり、前記認証サーバは、暗号化プログラムにより暗号化された第２のデータと、自身が保有する第２のデータを前記暗号化関数で暗号化したものと比較することにより前記ユーザー端末からのセッションの正当性を評価することを特徴とする請求項１記載のネットワーク認証装置。

3．前記暗号化情報は、前記ユーザー端末から仲介サーバへのセッション毎に変化することを特徴とする請求項１または２記載のネットワーク認証装置。

4．前記第１のデータはユーザーＩＤであり、第２のデータはパスワードであることを特徴とする請求項１記載のネットワーク認証装置。

5．前記暗号化情報は、前記認証サーバのかわりに前記仲介サーバが有する複数の暗号化関数の中から暗号化関数を特定する暗号化キーであることを特徴とする請求項２記載のネットワーク認証装置。

6．ユーザー端末より受信した第１のデータを仲介サーバにおいて認証サーバに仲介するステップと、

前記第１のデータに基づいて暗号化情報を生成し、当該暗号化情報を仲介サーバに送信するステップと、

前記第１のデータに対応し認証サーバが保有する第２のデータを読み出してこれを前記暗号化情報で暗号化するステップと、

仲介サーバにおいて、前記暗号化情報に基づいて、前記ユーザー端末で

入力される第２のデータを暗号化するための暗号化プログラムを生成し、この暗号化プログラムを前記ユーザー端末に配信するステップと、

ユーザー端末において、前記暗号化プログラムによって入力された第２のデータを暗号化するステップと、

ユーザー端末で暗号化された第２のデータを、前記認証サーバで暗号化された第２のデータと比較するステップとからなるネットワーク認証方法。

７．前記暗号化情報は、前記ユーザー端末から仲介サーバへのセッション毎に変化することを特徴とする請求項６記載のネットワーク認証方法。

８．ユーザー端末より受信した第１のデータを仲介サーバにおいて認証サーバに仲介するステップと、

前記第１のデータに基づいて暗号化情報を生成し、当該暗号化情報を仲介サーバに送信するステップと、

前記第１のデータに対応し認証サーバが保有する第２のデータを読み出してこれを前記暗号化情報で暗号化するステップと、

仲介サーバにおいて、前記暗号化情報に基づいて、前記ユーザー端末で入力される第２のデータを暗号化するための暗号化プログラムを生成し、この暗号化プログラムを前記ユーザー端末に配信するステップと、

ユーザー端末において、前記暗号化プログラムによって入力された第２のデータを暗号化するステップと、

ユーザー端末で暗号化された第２のデータを、前記認証サーバで暗号化された第２のデータと比較するステップとからなるプログラムを記憶した記憶媒体。

９．データを入力するユーザー端末に対して、当該データを仲介する仲介サーバと、当該データに対して認証を与える認証サーバとからなり、

前記ユーザー端末での処理要求の入力を契機に、前記処理要求に対する固有情報を発生させる認証サーバと、

前記固有情報に基づいて生成した入力インターフェースを前記ユーザー端末に提供する仲介サーバとからなるネットワーク認証装置。

１０．前記入力インターフェースは、ユーザー端末上で機能する実行プログラムであり、

当該実行プログラムは２以上のユーザー情報の入力を受け付けるとともに、

前記で入力された２以上のユーザー情報を暗号化して前記仲介サーバに送信する請求項９記載のネットワーク認証装置。

図 1

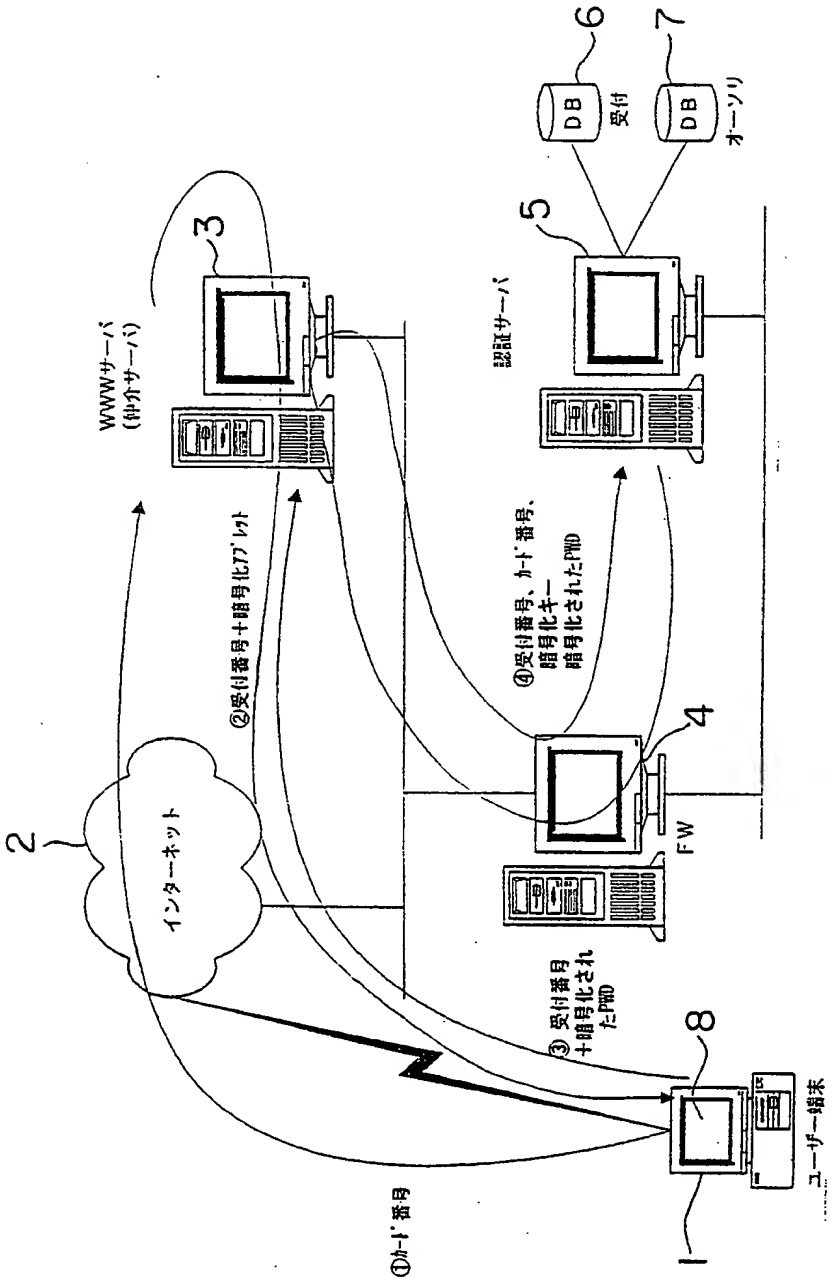

1
2
インターネット
3
WWWサーバ
(申介サーバ)
4
FW
5
認証サーバ
6
DB
受付
7
DB
オーソリ
8
ユーザー端末
①カード番号
②受付番号+暗号化アドレス
③受付番号
+暗号化された
PWD
④受付番号、カード番号、
暗号化キー
暗号化されたPWD

図 2

＜受付ＤＢ＞

受付番号	認証サーバで打番された受付のための番号
カードＩＤ	ユーザによって入力されたカード番号
暗号化キー	暗号化アルゴリズムを特定するためのキー

【図 3】

＜オーソリＤＢ＞

カードＩＤ	あらかじめ登録されているカード番号
パスワード	あらかじめ登録されているパスワード

図 4

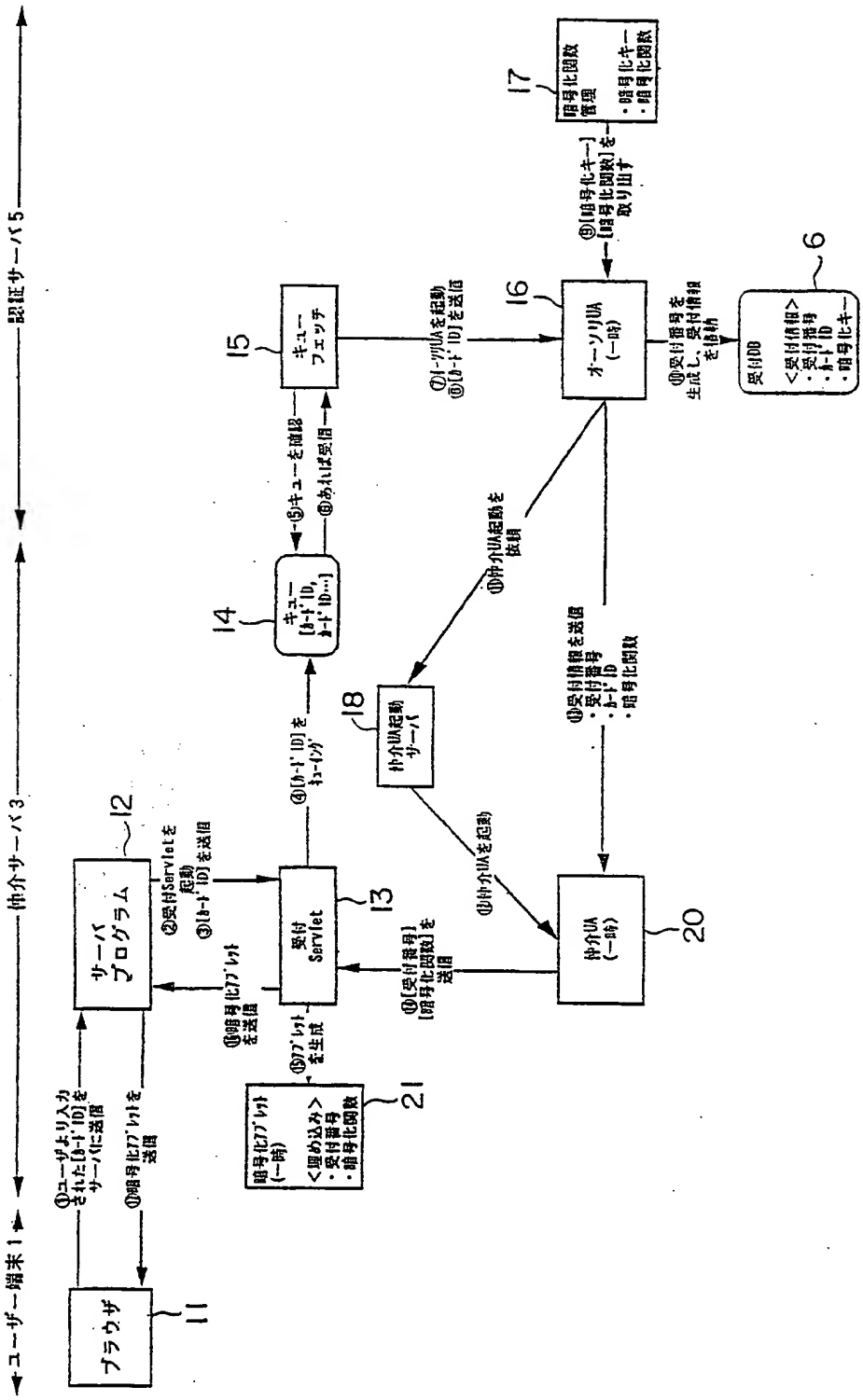

ユーザー端末 1
仲介サーバ 3
認証サーバ 5
ブラウザ
11
サーバプログラム
12
受付Servlet
13
キュー
[ﾕｰｻﾞｰID, ﾕｰｻﾞｰID…]
14
キューフェッチ
15
オーソリUA
(一時)
16
暗号化関数
管理
・暗号化キー
・暗号化関数
17
仲介UA起動
サーバ
18
仲介UA
(一時)
20
暗号化アプレット
(一時)
<埋め込み>
・受付番号
・暗号化関数
21
受付DB
<受付情報>
・受付番号
・ﾕｰｻﾞID
・暗号化キー
6
①ユーザより入力
された[ﾕｰｻﾞID]を
サーバに送信
②受付Servletを
起動
③[ﾕｰｻﾞID]を送信
④[ﾕｰｻﾞID]を
キューイング
⑤キューを問合
⑥あれば受信
⑦ｵｰｿﾘUAを起動
⑧[ﾕｰｻﾞID]を送信
⑨[暗号化キー]
[暗号化関数]を
取り出す
⑩受付番号を
生成し、受付情報
を登録
⑪仲介UA起動を
依頼
⑫仲介UAを起動
⑬[受付番号]
[暗号化関数]を
送信
⑭受付情報を送信
・受付番号
・ﾕｰｻﾞID
・暗号化関数
⑮暗号化ｱﾌﾟﾚｯﾄ
を送信
⑯ｱﾌﾟﾚｯﾄ
を生成
⑰暗号化ｱﾌﾟﾚｯﾄ
を送信

図 5

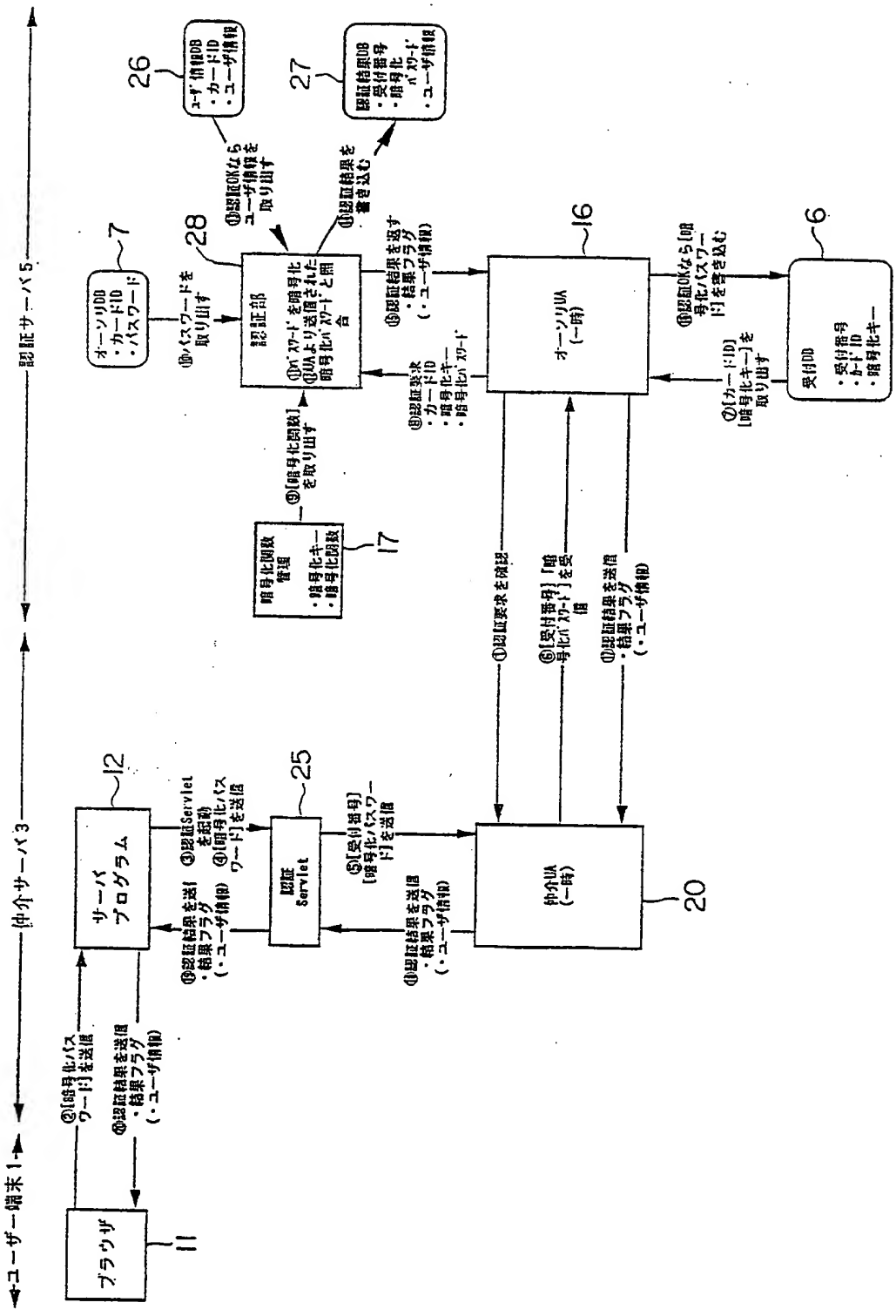

ユーザー端末 1
仲介サーバ 3
認証サーバ 5
ブラウザ
11
サーバプログラム
12
認証Servlet
25
仲介UA
(一時)
20
オーソリUA
(一時)
16
認証部
28
オーソリDB
・カードID
・パスワード
7
ユーザ情報DB
・カードID
・ユーザ情報
26
認証結果DB
・受付番号
・暗号化
パスワード
・ユーザ情報
27
受付DB
・受付番号
・カードID
・暗号化キー
6
暗号化関数
管理
・暗号化キー
・暗号化関数
17
②[暗号化パス
ワード]を送信
⑭認証結果を送信
・結果フラグ
(・ユーザ情報)
③認証Servlet
を起動
④[暗号化パス
ワード]を送信
⑬認証結果を送信
・結果フラグ
(・ユーザ情報)
⑤[受付番号]
[暗号化パスワー
ド]を送信
⑫認証結果を送信
・結果フラグ
(・ユーザ情報)
⑥パスワードを
取り出す
⑦[暗号化関数]
を取り出す
⑧[暗号化パス
ワード]と照
合
⑨認証OKなら
ユーザ情報を
取り出す
⑩認証結果を
書き込む
⑪認証結果を返す
・結果フラグ
(・ユーザ情報)
⑧認証要求
・カードID
・暗号化キー
・暗号化パスワード
①認証要求を確認
⑥[受付番号]「暗
号化パスワード」を受
信
⑫認証結果を送信
・結果フラグ
(・ユーザ情報)
⑬認証OKなら[暗
号化パスワー
ド]を書き込む
⑦[カードID]
[暗号化キー]を
取り出す

図 6

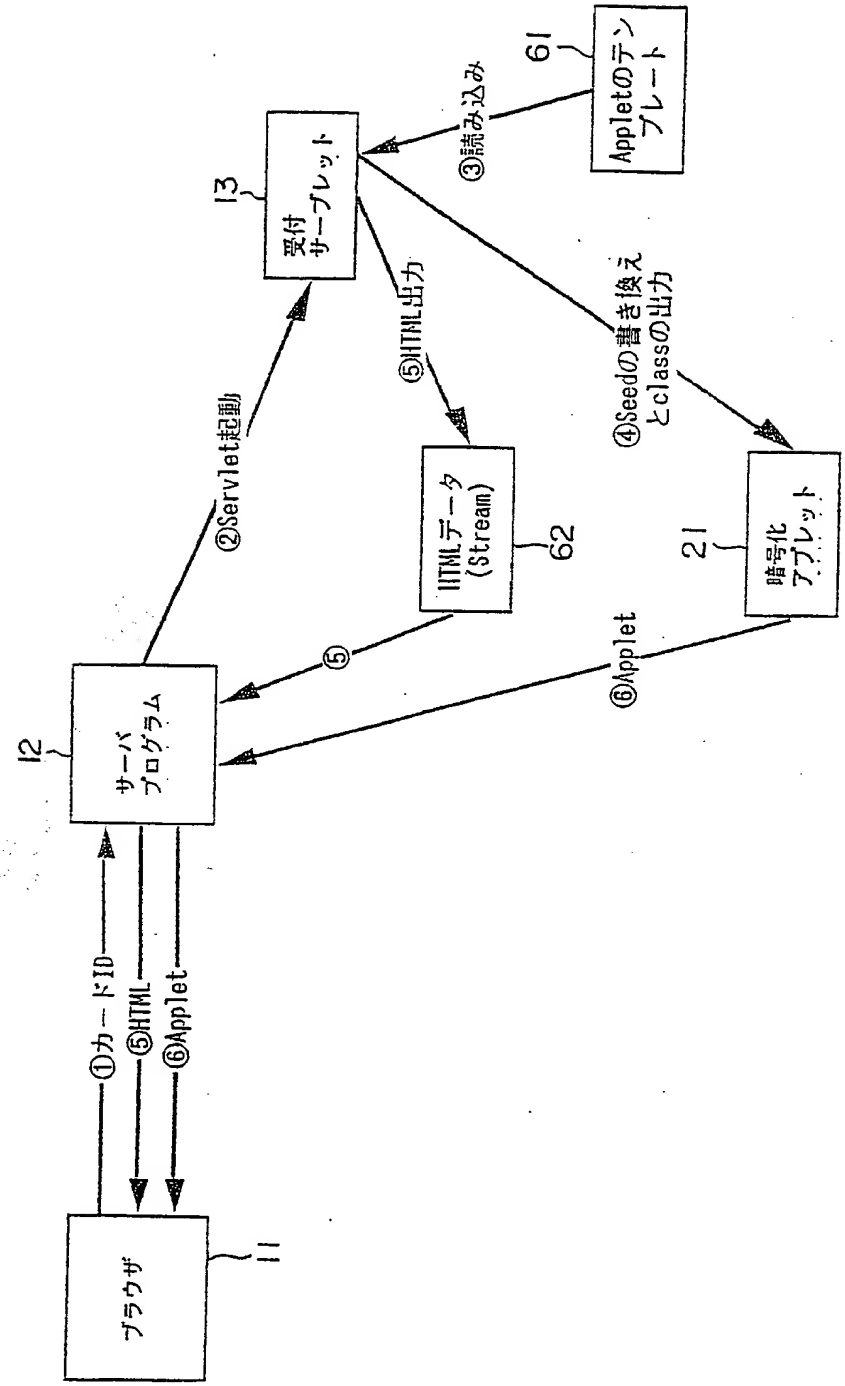

ブラウザ
11
サーバ
プログラム
12
受付
サーブレット
13
Appletのテン
プレート
61
HTMLデータ
(Stream)
62
暗号化
アプレット
21
①カードID
⑤HTML
⑥Applet
②Servlet起動
③読み込み
④Seedの書き換え
とclassの出力
⑤HTML出力
⑤
⑥Applet

図 7

```
<HTML>
<HEAD>
<TITLE>パスワード入力画面</TITLE>
</HEAD>
<BODY>

   . . . . . .

<APPLET CODE="OTP19980812114910.class" WIDTH=400 HEIGHT=300>
</APPLET>

   . . . . . .

</BODY>
</HTML>
```

62

図 8

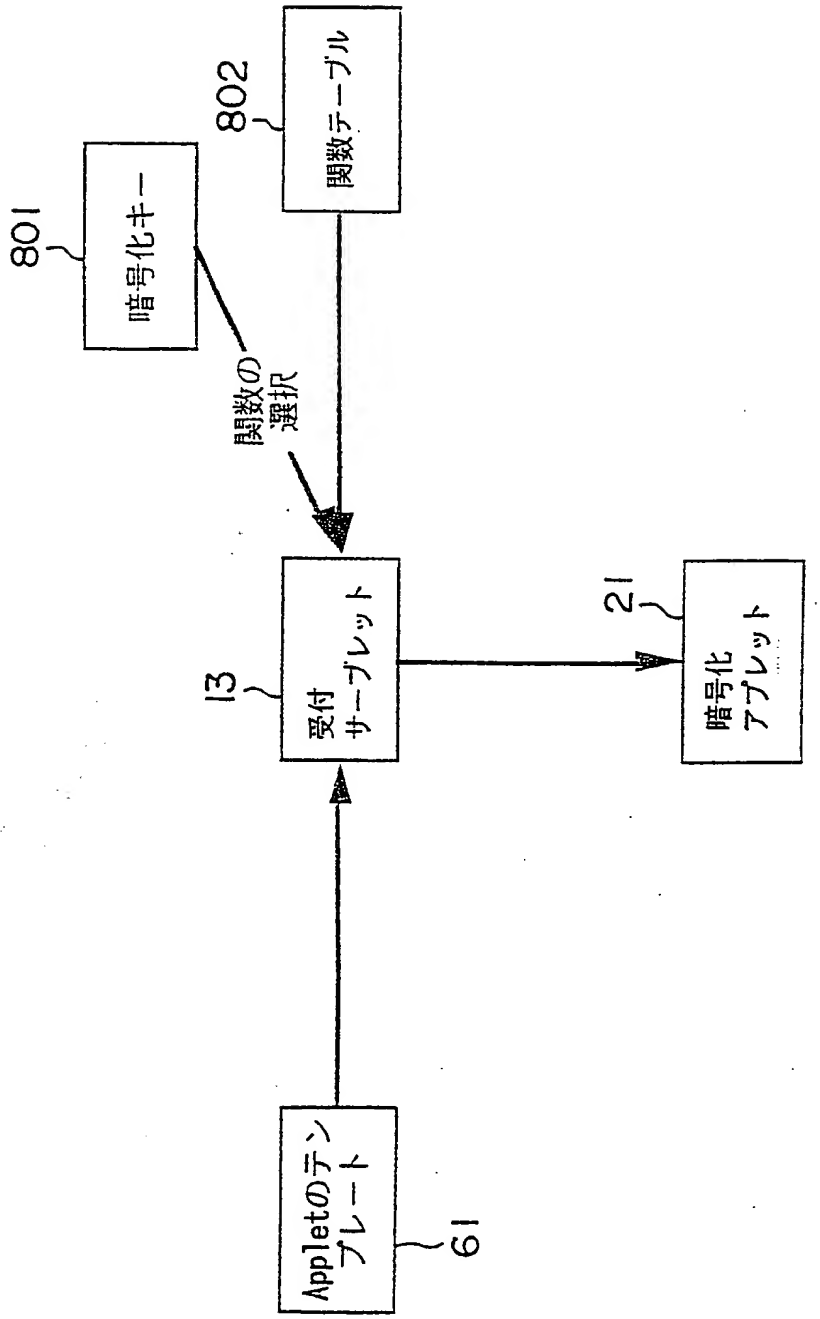

802
関数テーブル
801
暗号化キー
関数の選択
13
受付サーブレット
21
暗号化アプレット
Appletのテンプレート
61

図 9

table A

1	Y	=	a	X	+	2
2	Y	=	a	X	+	9
3	Y	=	a	X	+	3

a : マシン日付の日を使用する

図10

table B

4	Y	=	b	X	+	5
5	Y	=	b	X	+	7
6	Y	=	b	X	+	6

b : マシン日付の月を使用する

図１１

日付の下１桁が１，４，７	Ｙ ＝ ＡＸ ＋ Ｂ ＋ Ｃ
日付の下１桁が２，５，８	Ｙ ＝ (A+B) Ｘ ＋ Ｃ
日付の下１桁が３，６，９	Ｙ ＝ (A+C) Ｘ ＋ Ｂ
日付の下１桁が０	Ｙ ＝ (A＋B＋C)Ｘ ＋ Ａ

図１２

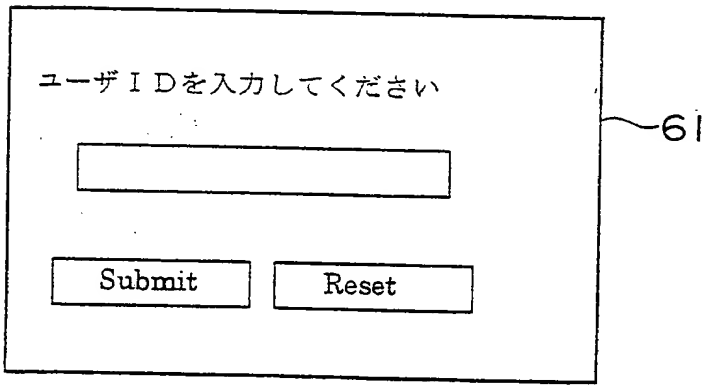
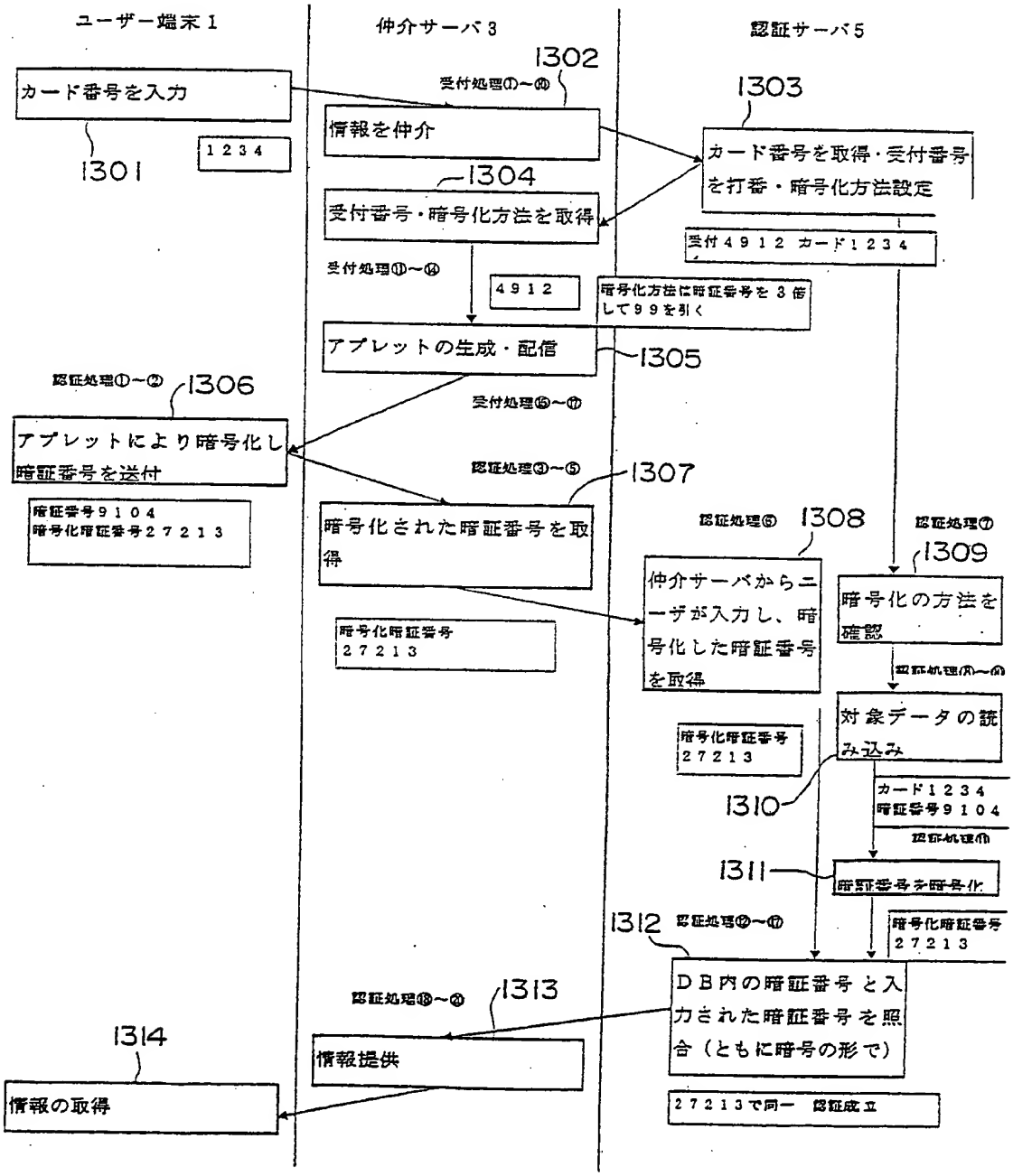


図１３


ユーザー端末１
仲介サーバ３
認証サーバ５
1302
受付処理①～⑩
1303
カード番号を入力
情報を仲介
カード番号を取得・受付番号を打番・暗号化方法設定
1234
1301
1304
受付番号・暗号化方法を取得
受付４９１２ カード１２３４
受付処理⑪～⑭
４９１２
暗号化方法に暗証番号を３倍して９９を引く
アプレットの生成・配信
1305
認証処理①～②
1306
受付処理⑮～⑰
アプレットにより暗号化し暗証番号を送付
認証処理③～⑤
1307
暗証番号９１０４
暗号化暗証番号２７２１３
暗号化された暗証番号を取得
認証処理⑥
1308
認証処理⑦
1309
仲介サーバからユーザが入力し、暗号化した暗証番号を取得
暗号化の方法を確認
暗号化暗証番号
２７２１３
認証処理⑧～⑩
対象データの読み込み
暗号化暗証番号
２７２１３
1310
カード１２３４
暗証番号９１０４
認証処理⑪
1311
暗証番号を暗号化
暗号化暗証番号
２７２１３
1312
認証処理⑫～⑰
ＤＢ内の暗証番号と入力された暗証番号を照合（ともに暗号の形で）
認証処理⑱～⑳
1313
情報提供
1314
情報の取得
２７２１３で同一 認証成立

This Page Blank (uspto)

図１４


簡易認証画面例 - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) 移動(G) お気に入り(A) ヘルプ(H)
中止 更新 ホーム
アドレス C:¥WINNT¥Profiles¥yamada¥デスクトップ¥簡易認証画面例.htm
○○カード会社ホームページ
ポイント照会
請求先登録
各種申請
店舗一覧

図１５

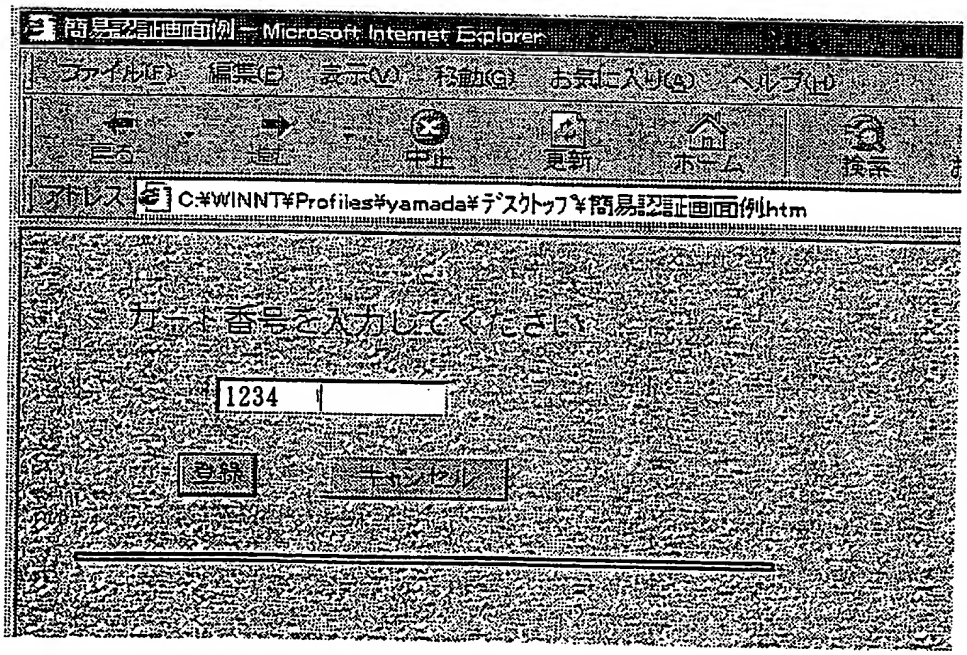

簡易認証画面例 - Microsoft Internet Explorer
ファイル(F) 編集(E) 表示(V) 移動(G) お気に入り(A) ヘルプ(H)
中止 更新 ホーム
アドレス C:¥WINNT¥Profiles¥yamada¥デスクトップ¥簡易認証画面例.htm
カード番号を入力してください
1234
登録
キャンセル

図１６

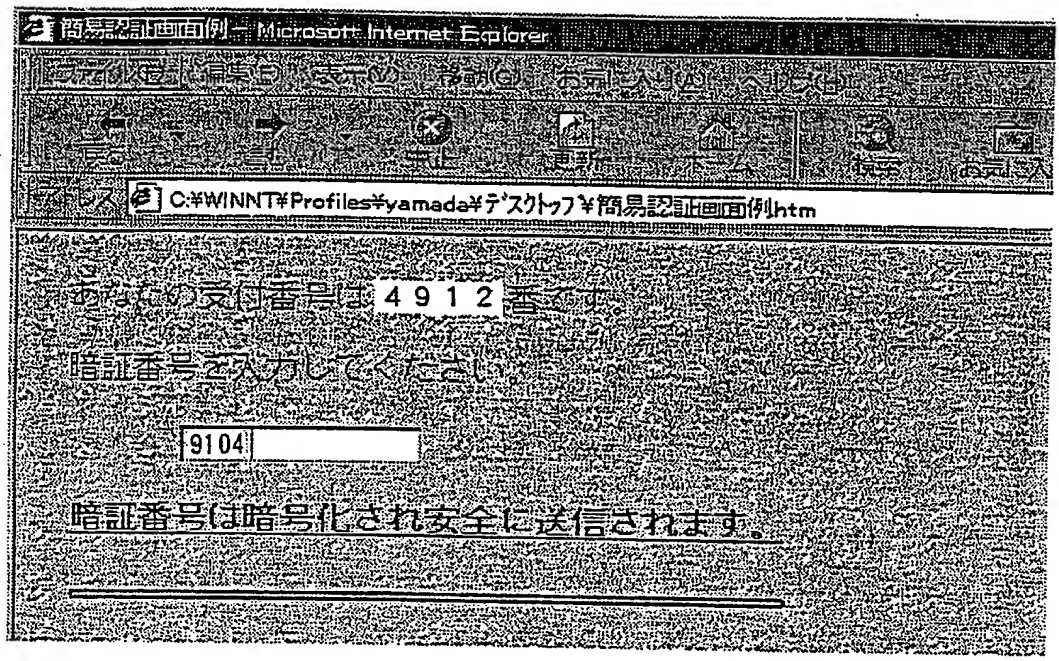

簡易認証画面例 - Microsoft Internet Explorer
C:¥WINNT¥Profiles¥yamada¥デスクトップ¥簡易認証画面例.htm
あなたの受付番号は 4912 番です。
暗証番号を入力してください。
9104
暗証番号は暗号化され安全に送信されます。

図１７

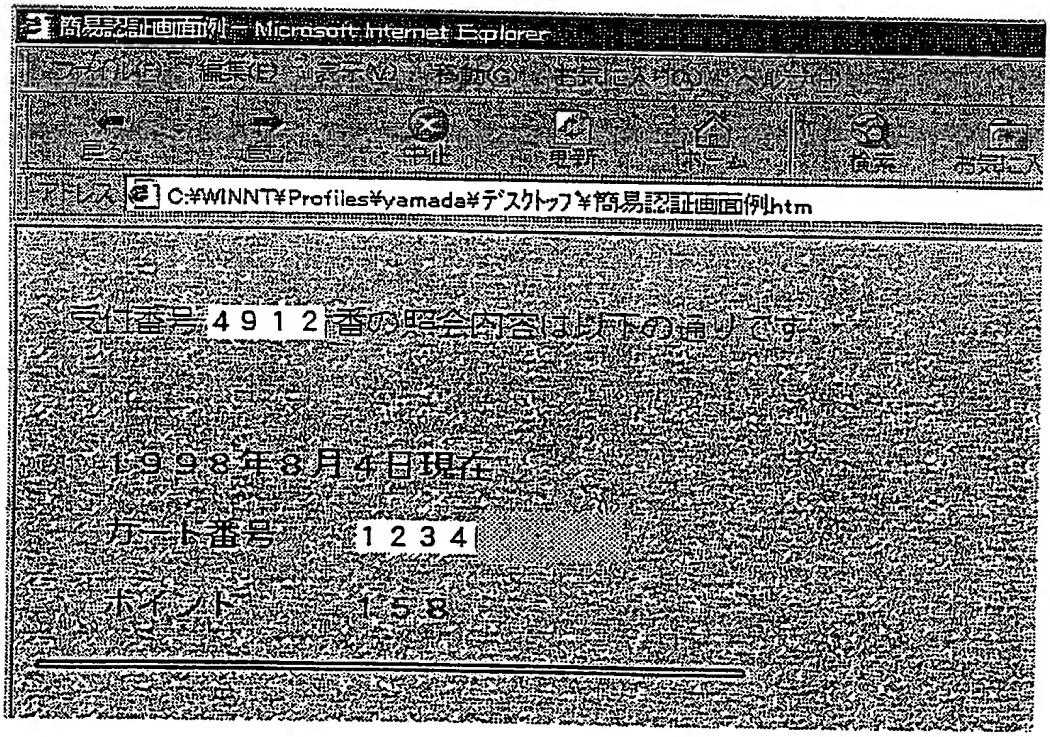

簡易認証画面例 - Microsoft Internet Explorer
C:¥WINNT¥Profiles¥yamada¥デスクトップ¥簡易認証画面例.htm
受付番号 4912 番の照会内容は以下の通りです。
1998年8月4日現在
カード番号 1234
ポイント 158

図１８

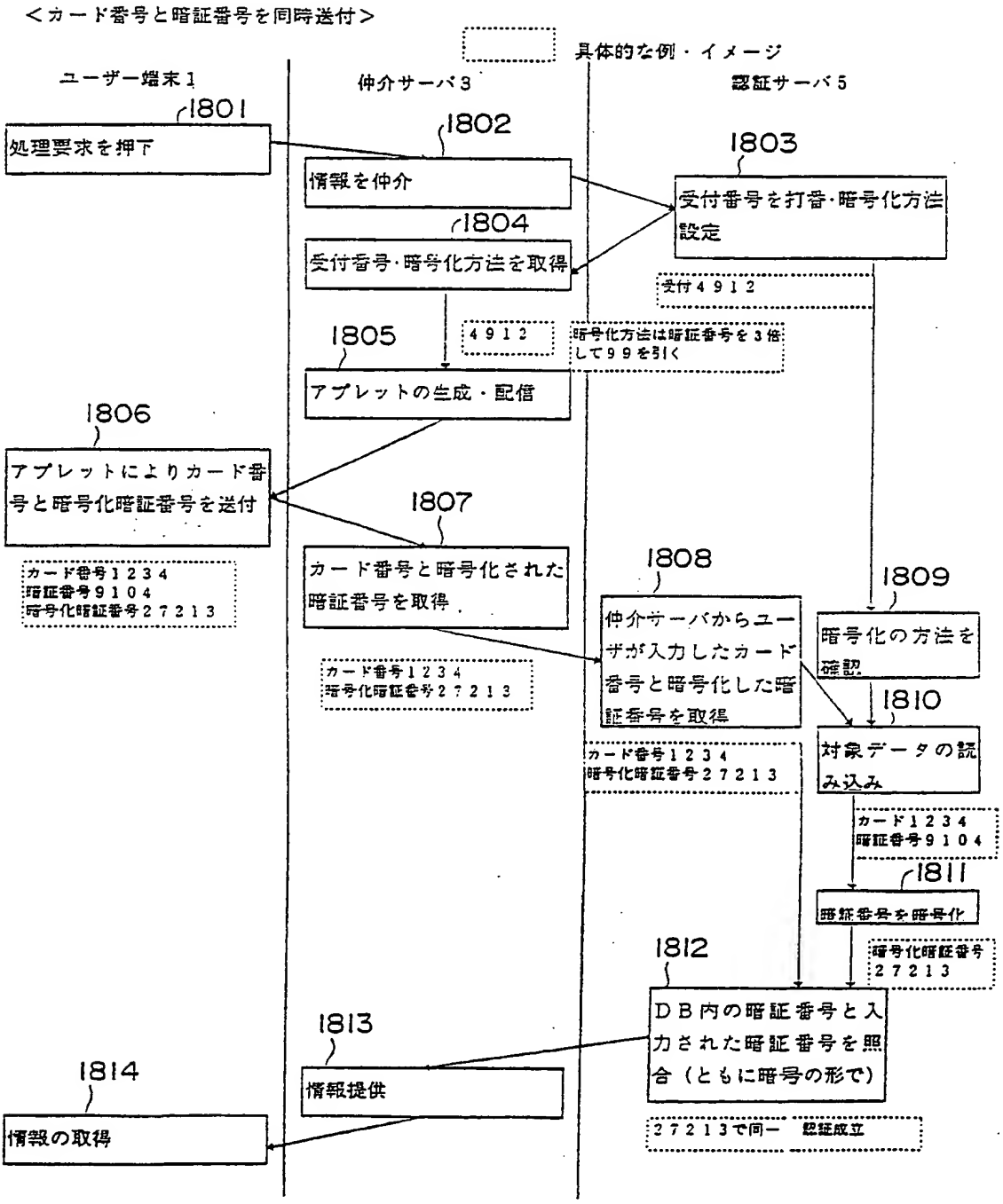
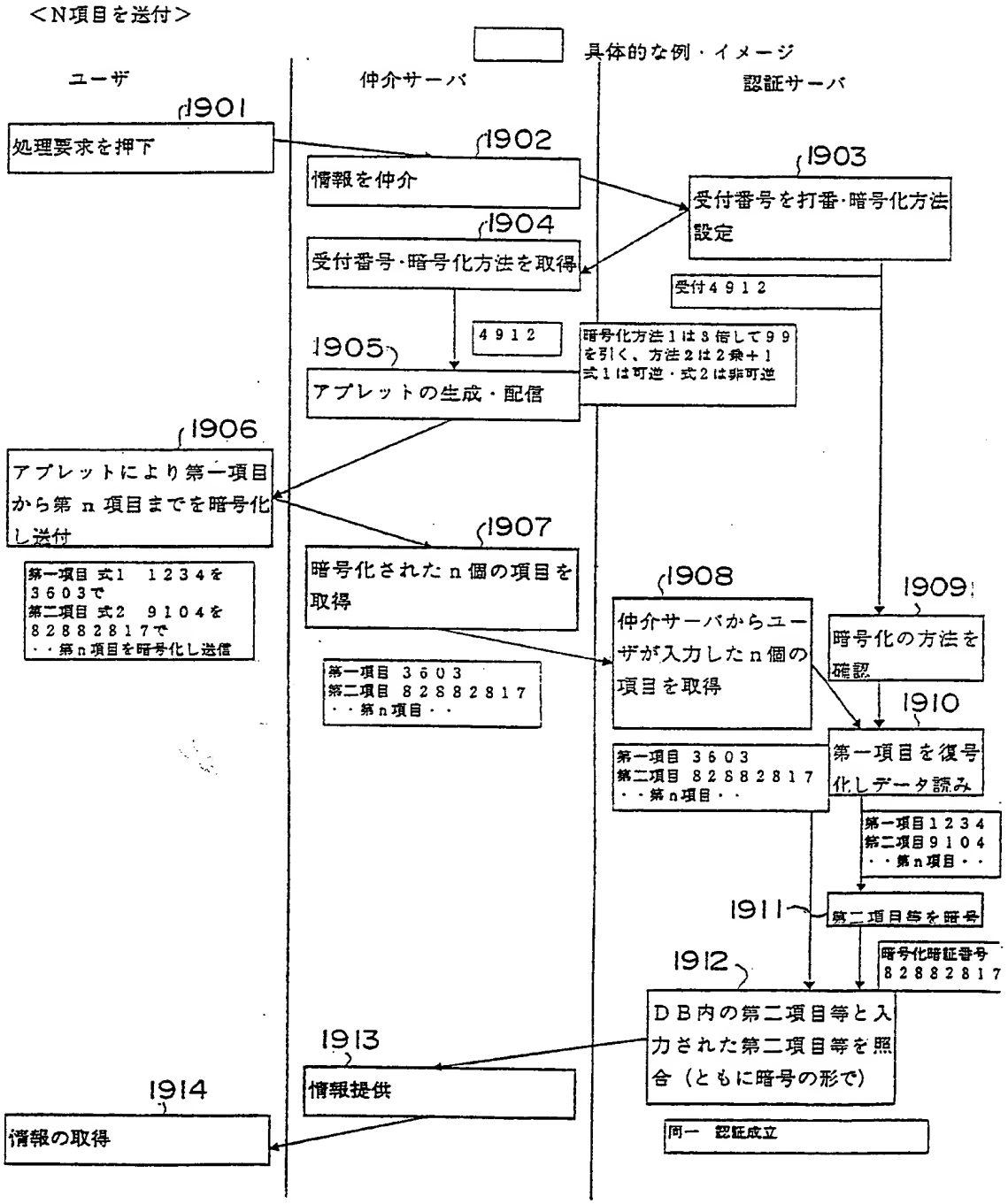

<カード番号と暗証番号を同時送付>
具体的な例・イメージ
ユーザー端末１
仲介サーバ３
認証サーバ５
1801
処理要求を押下
1802
情報を仲介
1803
受付番号を打番・暗号化方法設定
1804
受付番号・暗号化方法を取得
受付４９１２
４９１２
暗号化方法は暗証番号を３倍して９９を引く
1805
アプレットの生成・配信
1806
アプレットによりカード番号と暗号化暗証番号を送付
1807
カード番号と暗号化された暗証番号を取得
カード番号１２３４
暗証番号９１０４
暗号化暗証番号２７２１３
1808
仲介サーバからユーザが入力したカード番号と暗号化した暗証番号を取得
1809
暗号化の方法を確認
カード番号１２３４
暗号化暗証番号２７２１３
1810
対象データの読み込み
カード１２３４
暗証番号９１０４
1811
暗証番号を暗号化
暗号化暗証番号２７２１３
1812
ＤＢ内の暗証番号と入力された暗証番号を照合（ともに暗号の形で）
1813
情報提供
1814
情報の取得
２７２１３で同一　認証成立

図１９


<N項目を送付>
具体的な例・イメージ
ユーザ
仲介サーバ
認証サーバ
1901
処理要求を押下
1902
情報を仲介
1903
受付番号を打番･暗号化方法設定
1904
受付番号･暗号化方法を取得
受付４９１２
４９１２
暗号化方法１は３倍して９９を引く、方法２は２乗＋１式１は可逆・式２は非可逆
1905
アプレットの生成・配信
1906
アプレットにより第一項目から第ｎ項目までを暗号化し送付
第一項目 式１ １２３４を３６０３で
第二項目 式２ ９１０４を８２８８２８１７で
・・第ｎ項目を暗号化し送信
1907
暗号化されたｎ個の項目を取得
第一項目 ３６０３
第二項目 ８２８８２８１７
・・第ｎ項目・・
1908
仲介サーバからユーザが入力したｎ個の項目を取得
1909
暗号化の方法を確認
1910
第一項目を復号化しデータ読み
第一項目 ３６０３
第二項目 ８２８８２８１７
・・第ｎ項目・・
第一項目１２３４
第二項目９１０４
・・第ｎ項目・・
1911
第二項目等を暗号
暗号化暗証番号
８２８８２８１７
1912
ＤＢ内の第二項目等と入力された第二項目等を照合（ともに暗号の形で）
1913
情報提供
同一 認証成立
1914
情報の取得

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.